

digiCRYPT

mobile communication encryption software

User's manual v.2.1.en



Digitech, d.o.o., Podlimbarskega ulica 29, 1000 Ljubljana, Slovenia, EUROPE, www.digicrypt.info

CONTENTS

digicRYPT – the application description	3
digicrypt Installation	3
Using the XMPP server.....	3
digicRYPT application	4
digicrypt Main screen.....	5
Calling, Contacts list (Adress book)	5
the Wake-up SMS	6
Calling.....	6
Sending an encrypted SMS message	7
File transfer	8
Adding the new user	8
Logout and lock.....	8
Useful information about digicRYPT	9
Information about GSM bugging possibilities	9



DIGICRYPT – THE APPLICATION DESCRIPTION

digiCRYPT is an end-to-end VoIP encryption software solution for mobile phones. Application enables encrypted full duplex speech conversation and also text messages communication. Using digiCRYPT does not require any hardware upgrades on the mobile phone itself. For the encryption, 4096 bit RSA public and 256 bit AES private keys are used where the AES key is changed for every session/conversation.

For securing the voice and data information 3G/UMTS, GPRS/EDGE or WiFi networks can be used (data connection). There is an application available for personal computer as well (so call from GSM phone to PC is possible as well).

User name and password can be created on a public XMPP server or the user can create and use its own XMPP server. XMPP is used only to match device IP's addresses, all communication is direct device-to-device.



DIGICRYPT INSTALLATION

The .apk installation file must be send to mobile phone using PC or an installation file should be copied to the phone's SD card. If the file is copied to the phone, you must run this file using filesystem managing program (for example Astro manager) and the digiCRYPT application installation starts.

After the digiCRYPT software is installed, we can run it and log in using our user name and password. When we start the application for the first time, it takes pretty long to finish the initialization, because encoding keys (private and public) are generated during this (first) application startup.



USING THE XMPP SERVER

XMPP server is used in digiCRYPT application for initial IP exchanging. Simply said – the calling phone checks on XMPP server, which IP adress called phone has at the time of a call (IP addresses are usually changed with each GPRS/UMTS session). Afterwards all communication between phones is direct – so no call data is going through XMPP server at all.

An OpenFire XMPP server is suggested to be used with digiCRYPT system.

For testing (demo version) purposes only the Digitech's XMPP server will be allowed (@digicrypt.mobi), when having a full licence, we can use any XMPP server.



DIGICRYPT APPLICATION

We start the digiCRYPT application by starting it via the program shortcut.

At first application startup, we are prompted to select a PIN code, which we will use to access digiCRYPT program for further use. We must enter PIN twice in order to ensure that we entered it correctly. Any character (not only numbers) can be used for PIN password. Minimum allowed PIN length is 4 characters..

The PIN is used together with the phone unique ID to encrypt the application's settings (including the RSA private key).

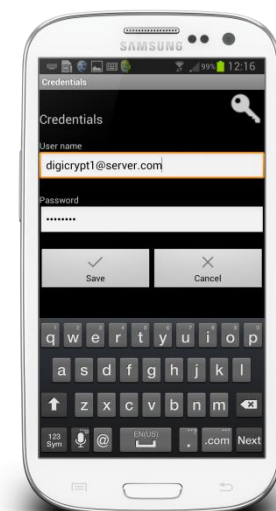
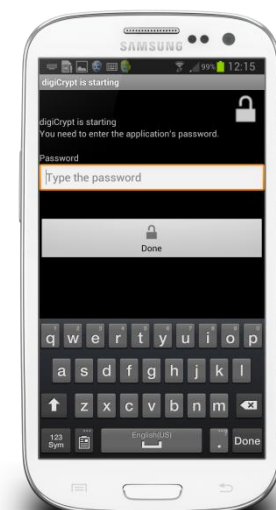
When we start the application for the next time, we are prompted to enter PIN number. If PIN is not entered, error message appears and the application does not start.

CAUTION!

PIN information is not stored anywhere! In case that you loose PIN code, access to the application is not possible and all application settings, contacts etc. cannot be obtained anymore by any means!

When the application starts, it tries to connect to the XMPP server and username and password for XMPP are requested. You should use username and password as set on XMPP server (username example: john.smith@digicrypt.mobi).

After clicking on a „Login“ button, the program connects to XMPP server and refreshes program's contact list.





DIGICRYPT MAIN SCREEN

After successful login the main screen opens, where we can navigate using finger for sliding the display up and down.

The top section contains all contacts, that we can communicate to („Contacts“) or the list of the last made calls („Log«). You can switch between both lists using bottom buttons.

Contacts that are **gray**, are currently **offline** (application is not running or does not have a connection to XMPP) and we can't talk to them directly (we can use „Wake up SMS“ function). **Contacts** which has **white icons** are **online** and we can call them by clicking on the username.

In a »Log«, button direction means call direction (in the phone: incoming, out of the phone: outgoing). The green color means successful connection and red color means no connection (for example, nobody answered the call).

If we **hold the contact for a while**, a menu for additional options opens (Send SMS, Edit, File transfer)



CALLING, CONTACTS LIST (ADDRESS BOOK)

When we click on the „online“ user, a window with the call button appears. With a click on the „Call“ button, a calling started.

If we hold the user for a while instead of clicking on it, „advanced user menu“ opens, where we can select „Edit“, »Delete«, „Send encrypted SMS“ or »Send encrypted file«. Those functions will be described further in the manuals.





THE WAKE-UP SMS

The „Wake up SMS“ can be used in a case, that the user with which we want to communicate is offline (not connected to the server). With „Wake up SMS“ we send him a SMS message where we ask him to start the digiCRYPT application (pre-defined SMS content: „Please launch digiCrypt“).

A phone number of the called user must be defined in order to make „Wake up“ function working. You can set it, if pressing „Edit“ button in the »Contacts« list.



CALLING

When we call selected contact, ringing starts. When a called person accepts the call securing incoming and outgoing call procedure starts, which takes few seconds (on display: securing incoming/outgoing). During this time, unique keys for the session encryption are created and exchanged between both sides.

After key exchange (when both conversation directions are secured) we can talk using phone as normal. After the conversation is over, we hang up the call with the on-screen „End call“ button. Signal strength bar indicator is also displayed during the conversation, which gives us estimate connection quality.

If this is the first time, that the contacts are in conversation, a key exchange must be preformed first and user is warned, that this is the first time, the user is communicating with the person called.

If this message appears on a contact, which has been called before, it means that its phone might be changed (application reinstall will cause certificate replacement) or the user's identity might be fraud (someone else is trying to communicate using this person's XMPP account). Be aware in such situations, that you check the reason for a different key!



Call quality in a great way depends on a (mobile or WLAN) network quality. If network speed is insufficient, a gaps in the conversation may occur or call is even terminated. Please make sure, that a network signal is sufficient. (network bar graph on phones refresh rate is pretty slow, so it may not shows the real status).



SENDING AN ENCRYPTED SMS MESSAGE

If we want to send an encrypted message to the user, we must hold the user until „advanced user menu“ opens, then select „Encrypt SMS“ button.

The window opens, where we can enter the text we would like to send and then press „Send SMS“ button.

For receiving an encrypted SMS message, we simply click on the URL, that is in the standard message. This way the digiCRYPT program will decrypt and display the message.

The user, to which we want to send encrypted SMS can be online (logged into digiCRYPT) or offline – he will receive encrypted message as standard SMS message!

Before the first message exchange, we must do at least one call to the other person, so the certificate exchange is preformed.

In case that we haven't established a communication with the other party yet, the error message will be displayed.





FILE TRANSFER

digiCRYPT enables also encrypted file transfer, which can also be done through the »Contacts« list. Holding down the contact and selecting »Send encrypted file« brings up the file select window, where we can select a file to transfer and confirm sending.

When a receiver gets a incoming file notification, this notification must be confirmed and the file transfer begins.

Before the first file exchange, we must do at least one call to the other person, so the certificate exchange is preformed.

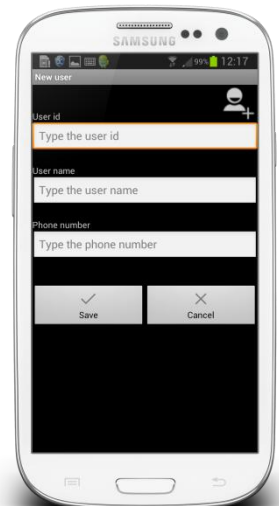
In case that we haven't established a communication with the other party yet, the error message will be displayed.



ADDING THE NEW USER

When adding new contact, at least „User account“ name must be entered.

Other two parameters (Visible user name, Phone number) are optional, but we suggest you entering phone number as well in order to have „Wake up SMS“ and „Encrypted SMS“ functions enabled.



LOGOUT AND LOCK

Using „Logout and lock“ button, we minimize and close the digiCRYPT program. To bring the program on the screen again, press the program icon. To shut down the program completely, close it via Program manager app.





INFORMATION ABOUT GSM BUGGING POSSIBILITIES

The digiCRYPT application ensures highest level encryption for the phone conversation. The conversation is secured all the way between both phones included in the conversation, so also in a case of data interception voice data is secured.

However, we must warn about the possibility of bugging using voice bugs in the area, where a call is made. Such bug can record/transmit the audio from the area, where we talk over the phone, so for the highest security we suggest communicating outside areas, where voice bugs can simply be placed (apartment, office, car ...).

Another possible way to intercept a secured call is some malware („virus“) on the phone, which can take control over microphone and speaker of the mobile phone (in-the-middle attack), so we suggest not to install any suspicious software on the mobile phone, where digiCRYPT is running.

